VZCZCXRO1443
OO RUEHBI RUEHCI
DE RUEHNE #4255/01 1671219
ZNR UUUUU ZZH
O 161219Z JUN 06
FM AMEMBASSY NEW DELHI
TO RUEHC/SECSTATE WASHDC IMMEDIATE 5414
INFO RUEHBJ/AMEMBASSY BEIJING 2554
RUEHIL/AMEMBASSY ISLAMABAD 8880
RUEHLO/AMEMBASSY LONDON 0334
RUEHKO/AMEMBASSY TOKYO 3474
RUEHCI/AMCONSUL CALCUTTA 4728
RUEHCG/AMCONSUL CHENNAI 4687
RUEHBI/AMCONSUL MUMBAI 3928
RUEAHLC/HOMELAND SECURITY CENTER WASHINGTON DC
RHEHNSC/NSC WASHDC
RUEIDN/DNI WASHINGTON DC
RHHMUNA/CDR USPACOM HONOLULU HI
RUCNDT/USMISSION USUN NEW YORK 1231
RHMFISS/HQ USCENTCOM MACDILL AFB FL
RUEHGV/USMISSION GENEVA 3525
RHHMUNA/HQ USPACOM HONOLULU HI
RHMFISS/HQ USSOCOM MACDILL AFB FL
RUEKJCS/JOINT STAFF WASHDC

UNCLAS SECTION 01 OF 05 NEW DELHI 004255

SIPDIS

SENSITIVE
SIPDIS

STATE FOR PM/PPA

E.O. 12958: N/A
TAGS: PREL PGOV KCIP TINT PINR IN
SUBJECT: FOLLOW-UP WITH CERT-IN: COOPERATIVE APPROACH TO ADVOCATING CYBERSECURITY

REF: A. NEW DELHI 1670
¶B. 04 NEW DELHI 6953

¶1. (SBU) Summary: PolOff on June 6 revisited India's Computer Emergency Response Team (CERT-In) for the third time, with SciCouns and EconOff accompanying. CERT-In is pursuing a multi-platform outreach program to cybersecurity experts in the public, private, and academic sectors. Although last year phishing attacks were the most prevalent incident CERT-In handled, web defacement has been a top-level concern in the Indian cyber-community for several years. CERT-In Director Dr. Gulshan Rai reiterated throughout the tour his focus on cooperative or "soft" cybersecurity with purely domestic Internet entities in commerce, government, and academia; however, regarding Indian Internet players whose headquarters are in the US (and who he believes are insufficiently accommodating to his requests for subscriber data), he advocates a rules-based or "hard" approach. CERT-In's training classes are typically full, but they have no plans to offer distance learning to expand their educational reach. Rai also described his workforce, and complained about factors common to the IT industry that force him to accommodate nearly 100% annual staff turnover. End Summary.

CERT-In Briefing

¶2. (U) CERT-In Operations Director Anil Sagar narrated a ten-minute PowerPoint briefing of CERT-In operations. Highlights included:

-- CERT-In focuses on protecting critical data infrastructure for the defense, financial, energy, transportation, and telecommunications sectors.

-- CERT-In is working toward ISO/IEC 27001 information security management standards certification. It has drafted its informtion security management manual and expects

certification by December 2006.

-- CERT-In currently has no direct enforcement powers; if it chooses to follow up on computer security infractions committed by GOI entities, it must report up to the (Communications and Information Technology or C&IT) Ministry level. As regards the private sector, CERT-In is only empowered to issue voluntary cybersecurity guidelines, which Sagar described as "up to international standards."

Outreach

¶3. (U) CERT-In connects with digital India through multiple vectors:

-- Their web site www.cert-in.org.in generates an average of 460 hits/day from GOI, state governments, industry, and academia (including foreign institutions). Their web traffic is approximately 75% domestic and 25% from non-Indian sources.

-- In the past 18 months, they recorded 60,000 downloads of security guidelines and white papers from the web site. A large (but not quantified) number of downloads are executed from academic institutions in India, the US, and the UK.

-- Vulnerability Notes are e-mailed to a list of 550 data security professionals, including 125 CIOs.

-- Their e-mail contact list (for training and special events) includes 800 Indian CIOs in critical sectors (defense, finance, energy, transportation, telecomms) and

sub-sectors (banking, insurance, fertilizer, oil, power, etc.).

-- CERT-In is available for contact essentially 24/7 by phone, fax, and e-mail, though their graveyard shift is limited to one engineer at present.

Breakdown of Incidents Handled by CERT-In

¶4. (U) Sagar continued that of the total number of incidents CERT-In engineers worked on in 2005, 40% involved phishing attacks. Of the remainder:

-- 38% were virus/malicious code attacks

-- 16% were network scanning/probing incidents

-- 2% involved system misuse

-- 2% were e-mail spoofing

Web Defacements a Concern

¶5. (U) Sagar said that India's on-line community suffers from a significant amount of web defacements -- hacking to change the appearance of a corporate or governmend web site without also attacking back-end functions such as databases, e-commerce, etc. CERT-In has published two white papers on web defacement, both available through their web site. Highlights, including an analysis of data up to December 2004 as well as a simple graph of 2005 incidents, are:

-- Total annual web defacements of Indian sites logged by CERT-In since 2003 are: 1687 (2003), 1529 (2004), 4705 (2005), 899 (2006, first six months)

-- Almost half of the web defacement complaints CERT-In received in 2004 were from .co.in domains; .gov.in domains accounted for one-quarter of defacements, followed by academia (.ac.in) with one-eighth. India's remaining seven

domains, including .mil.in, shared equally in the remainder of defacements.

-- Telecomms networks and Internet infrastructure were the most targeted sites in 2004. The prior white paper noted a prevalence of defacements in past years against sites related to the railways and to the Gujarat state government.

-- The 2005 figures were 60% against .com domains and 10% against .org domains.

Advocating a Soft Approach with Indian Firms ...

¶6. (SBU) Asked by EmbOffs several times about how and under what authority CERT-In can enforce cybersecurity on the private sector, Rai continually relied on a mantra of "we seek voluntary compliance." Rather then confront firms and make enemies, it is better to educate them and convince them it is in their (financial) interest to follow good cybersecurity practices, he maintained. Rai said he finds that that in many cases the private sector (which understands that breaches of data security translate into costly fixes and potentially lost clients) is generally more appreciative, more forward-leaning, and more accommodating than GOI offices.

¶7. (SBU) Rai also shared that CERT-In receives tip-offs from industry insiders, whistle-blowers within firms and departments, and through the media, of companies and agencies

not adhering to cybersecurity best practices or suffering attacks. He reported that 60% of the entities CERT-In follows up with comply with their requests for information; their second-round requests that include a warning of possible legal infractions that might require a CBI investigation generate additional compliance, though he hastened to add that CERT-In had never referred a case of non-compliance or an attack to Indian law enforcement. Rai told us he has lobbied for amendments to the IT Act (2000) that would grant CERT-In the authority to directly issue cybersecurity mandates.

Frustrated with Procedural Inefficiency

¶8. (SBU) Rai's dander rose as he described his frustration over not being able to obtain Microsoft Hotmail and Yahoo personal subscriber data for e-mail accounts CERT-In has identified as having attacked CERT-In's own servers. He said that they have logged approximately 25 attacks against the facility this year, of which 10 were identified as US-origin, five Indian-origin, and the remainder spread among several other countries. Rai never singled out Pakistan as the origin of any attacks on CERT-In or other Indian servers, but he did note that some cyber-attackers located in one country hijack servers in another to launch attacks.

¶9. (SBU) Rai held to his position that the two companies should share the subscriber information directly with CERT-In despite EmbOffs' suggestion that the request -- if related to criminal activity -- could be pursued through law enforcement channels. "I keep asking the Indian headquarters for information, and they throw up their hands and say their US bosses won't let them help," he expounded, nearly choleric. When EconOff offered that US privacy rights were an important factor, Rai snapped, "They are criminals, why protect their privacy?"

Training: SRO, No Plans for Distance Ed

¶10. (SBU) CERT-In continues to run 2-day seminars and workshops, though no more than one training event per month. Some events, such as a CIO-level seminar that included an ICAAN executive as a speaker, overcrowd the facility's

24-seat seminar room -- this event yielded a crowd of "around 40, standing room only." Rai said they sometimes replicate seminars and workshops at IIT/Bangalore, but CERT-In has no plans to introduce distance learning; the conference room boasts videoconferencing equipment, but not the classroom, which is in the next room over. (COMMENT: Although hands-on workshops, which use CERT-In's networked and pre-loaded computer workstations, may be impractical for distance learning, EmbOffs were struck that CERT-In did not offer seats to over-subscribed seminars through teleconferencing. End Comment.)

Like IT Industry, Suffering High Turnover

¶11. (SBU) Rai and Sagar bemoaned CERT-In's high turnover rate of approximately 100% per year; Rai explained that employees' experience and connections are highly sought after by Delhi's growing private-sector IT industry, and that the director of Japan's CERT tried to hire away one of his employees. Rai also took a swipe at "changing cultural values" (read: Indian IT professionals act like their American counterparts). Young employees do not feel emotionally attached to their first job and can be easily snapped up by a better offer -- there is no social benefit to staying with one organization for years at a time, he

complained. Rai also noted that the security of the government sector is not as attractive as better salaries in the private sector, especially for IT professionals possessing portable skills. He added that Indian youth today willingly trade stability for mobility.

Platform-Driven Work Teams

¶12. (SBU) CERT-In staff are organized into work groups based on the platforms the engineers specialize in (Windows, Linux, Oracle, etc.). Members of a work group may work any number of the following tasks within their platform expertise:

-- Real-time or e-mail customer assistance

-- Resource building, including internal training and accumulating security tools, patches, and network technology

-- Event monitoring/incident handling and drafting/posting security alerts in response to newly discovered malware

-- Collecting data

-- Drafting/conducting training modules for CERT-In workshops

-- Trend analysis

-- Drafting white papers

-- Reverse-engineering malicious code

-- Conveying information to regional/international CERTs (AP Cert, CERT-CC) or coordinating/setting up Indian sector-specific CERTs

24 Hours a Day

¶13. (SBU) CERT-In currently employs 22 staff members divided into two main shifts, with a single person staffing the graveyard shift. Half the workforce are hired "from the market," while half are on deputation from other GOI departments. All have engineering or computer science degrees, including some MS and PhD holders. Rai told us the C&IT Ministry approved an increase up to 38 staff members, which would allow them to stand up a complete third shift. CERT-In augments its limited R&D manpower by enlisting help

from IIT and IIS computer science departments. CERT-In's partnerships with Microsoft, Cisco, Computer Associates, and Red Hat are force multipliers that allow CERT-In to outsource some projects, and Rai is also pursuing tie-ups with Symantec, Sun, HP, Juniper, Intel, AMD, McAfee, TrendMicro and IBM. (COMMENT: Rai easily separated his positive view of Microsoft regarding its Security Cooperation Program from his frustration with Microsoft noted in Para 7. End Comment.)

Security: Less Than Meets the Eye?

¶14. (SBU) Paying closer attention to CERT-In's security apparatus than in prior visits, we noticed several apparent lapses/inconsistencies:

-- We noticed biometric fingerprint-readers at six-eight doorways; in approximately half the cases, the doors had been propped open. Only when Sagar entered the NOC was a fingerprint read required.

-- The large number of CCTV cameras, badge-readers, and bio-metric sensors appear to be a security overkill --

perhaps more for show than for security -- considering that the physical space CERT-In occupies could not easily accommodate more than 40-50 per shift, plus up to 25 visitors/seminar attendees.

-- The X-Ray machine in the foyer still appears unused (Ref A).

Cybersecurity Audits Fell by the Wayside

¶15. (SBU) To PolOff's question on whether the RBI ever mandated cybersecurity audits (Ref B), Rai said that the mandate had never materialized. Instead, CERT-In offers voluntary cybersecurity audits to the private sector, performed by their staff engineers.

Breakdown of Hardware

¶16. (SBU) Further to Ref B, CERT-In's Network Operations Center (NOC) employs 10 Sun servers (two each labeled "Firewall" and "e-mail," six labeled "Web." The remainder of their servers are IBM.

¶17. (U) Visit New Delhi's Classified Website:
(http://www.state.sgov.gov/p/sa/newdelhi/)
MULFORD